REMARKS

1) Summary of Office Action

Claims 1 to 27 are pending in this application.

In the Office Action mailed May 20, 2004, the Examiner rejected claims 1 to 18 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,854,759 to Kaliski, Jr. *et al* (herein "Kaliski"). The Examiner rejected claims 19 to 24 under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,446,205 to Lenstra (herein "Lenstra"). The Examiner rejected claims 25 to 27 under 35 U.S.C. 103(a) as being obvious over Lenstra and further in view of Kaliski.

The Applicant traverses the Examiner's rejections as follows.

2) Remarks Concerning Amendments to the Specification

The specification is amended to correct several typographical errors. No new matter is introduced by these amendments.

3) Remarks Concerning Claim Amendments

Claims 1, 12 and 19 are independent claims. The Applicant amends claims 1 and 12 to recite a method for information exchange between a pair of correspondents exchanging cryptographic data. Claim 1 is further amended to recite that the converted element in a step of the method is further operated to obtain a result for use in exchanging cryptographic data with the second correspondent.

4) Anticipation - 35 USC 102(e) - (Claims 1 to 18)

The Examiner objected that claims 1 to 18 are anticipated by Kaliski. The Applicant respectfully traverses the objections as follows.

Claim 1 is an independent claim. It recites, among others, "forwarding said converted element to the first correspondent; and operating on said converted element by said first

correspondent in a cryptographic operation to obtain a result of said cryptographic operation for use in exchanging cryptographic data with said second correspondent."

Referring to Figure 13 of Kaliski, the Examiner stated, in part, that "[t]he enhanced arithmetic unit 160 includes the import basis converter 152 and is rotate/extract basis converter 154 described in conjunction with FIG. 12, as well as a finite field arithmetic unit 162 such as the arithmetic unit 50 of FIG. 4. The enhanced arithmetic unit 160 supports finite field arithmetic operations in an internal basis as well as an additional basis, and may include more than the one set of basis converters shown, whereby 'forwarding said converted element to the first correspondent' is considered to include in this arithmetic operations (column 16, lines 56-66)." Namely, the Examiner seemed to have equated multiple basis converters in enhanced arithmetic unit 160 to multiple correspondents and equated any possible communications between these internal basis converters to "forwarding said converted element to the first correspondent."

However, in Figures 12 and 13, it is clear that each set of the basis converters (one is shown) includes an import basis converter 152 and rotate/extract basis converter 154. Import basis converter 152 takes as its input a first basis representation and converts it to an internal representation. The element in the internal representation is further converted by rotate/extract basis converter 154 to a second basis representation. In this arrangement, two internal converters of a single basis converter, working in tandem, convert an element from one base to another.

While it is not entirely clear from Figure 13 of Kaliski whether the output of any of the multiple sets of basis converters of enhanced arithmetic unit 160 is in fact forwarded to any of other of the multiple sets of basis converters of enhanced arithmetic unit 160, it is clear from Figure 13 that the converted element is not forwarded back to a first correspondent from which the intermediate processor receives an element in a first basis as input. This is consistent with the objective and teaching of Kaliski. Kaliski addresses the problem of performing basis conversion in a resource limited system by improving speed of the algorithm and reducing memory requirement. The clear teaching of Kaliski is to continue to perform the basis conversion in a constrained environment (see also col. 10, lines 23 to 51). There is no teaching in Kaliski that the converted result is forwarded back to the first correspondent for use in exchanging cryptographic data with a second correspondent at all.

Further, none of the basis converters of Kaliski performs a cryptographic operation or exchanges cryptographic data with a second correspondent. Even if Kaliski, by disclosing that enhanced arithmetic unit 160 may include more than the one set of basis converters, suggests that the converted element is forwarded back to another one of basis converters, which the Applicant strongly disagrees, Kaliski does not disclose at all that the other basis converter performs a cryptographic operation on the converted element and uses the result for exchanging cryptographic data with another correspondent.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Further, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As Kaliski does not disclose each and every element as set forth in claim 1, let alone showing the invention in as complete detail as is contained in claim 1, it is submitted that the subject matter of claim 1 is not anticipated by Kaliski. Accordingly, the Applicant respectfully submits that claim 1, as amended, is patentable over Kaliski.

Similarly, claim 12 is an independent claim and recites, among others, "forwarding said first converted element to said second correspondent; and forwarding said second converted element to said first correspondent."

As submitted above, Kaliski discloses, in Figures 12 and 13 and the disclosure, that two internal converters of a single basis converter, working in tandem, convert an element from one base to another. Although Kaliski discloses that enhanced arithmetic unit 160 may include more than the one set of basis converters, there is no teaching, disclosure, or suggestion that the first converted element is forwarded to the second correspondent and the second converted element is forwarded to the first correspondent.

As Kaliski does not disclose each and every element as set forth in claim 12, let alone showing the invention in as complete detail as is contained in claim 12, it is submitted that the

subject matter of claim 12 is not anticipated by Kaliski. Accordingly, the Applicant respectfully submits that claim 12, as amended, is patentable over Kaliski.

Claims 2 to 9 and 13 to 18 depend, directly or indirectly, from either of independent claims 1 and 12. To the extent that claims 1 and 12 are presently allowable, claims 2 to 9 and 13 to 18 are also allowable.

5) **Anticipation - 35 USC 102(e) - (Claims 19 to 24)**

The Examiner objected that claims 19 to 24 are anticipated by Lenstra. The Applicant respectfully traverses the objections as follows.

Claim 19 is an independent claim. It recites, among others, "computing a first function of a first sequence of traces of said first field element."

Referring to Figure 5, the Examiner stated, in part, "[a]t step 515, the participant's cryptosystem randomly selects a bitstring s having Bs bits, that is for 'computing a first function of a first sequence of traces of said first field element'".

However, "trace" is a well-defined concept. See, for example, paragraph 20 of the present application. A "randomly" selected bitstring having a fixed number of bits is not a trace function of a field element. Accordingly, Lenstra does not disclose "computing a first function of a first sequence of traces of said first field element."

For at least this reason, it is respectfully submitted that claim 19 is not anticipated by Lenstra and is patentable over Lenstra.

To the extent claim 19 is patentable over Lenstra, it is respectfully sumitted that claims 20 to 24, depending from claim 19 directly or indirectly, are also patentable over Lenstra.

6) **Obviousness - 35 USC 103(a) - (Claims 25 to 27)**

Claims 25 to 27 depend from claim 19. The Examiner was of the view that Lenstra teaches the claimed subject matter except what is recited as further limitations in these dependent

claims. The Examiner was further of the view that the subject matter of these further limitations is taught by Kaliski.

However, as submitted above, Lenstra does not disclose each and every limitation of claim 19. Therefore, Lenstra and Kaliski, in combination, do not disclose each and every limitation of any of claims 25 to 27.

According to MPEP §2142, "The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness." Further, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

As Lenstra and Kaliski, in combination, do not teach nor suggest all the claim limitations of any of claims 25 to 27, the Applicant submits that the Examiner has failed to establish *prima facie* obviousness of a claimed invention and therefore claims 25 to 27 are patentable over Lenstra and Kaliski.

7) Closing Remarks

No new matter is introduced by the amendments provided herein. In light of the foregoing, the Applicant submits that the claims pending in this case are presently in a condition for allowance. As such, Applicant requests early and favourable disposition of this application.

Should the Examiner wish to discuss this matter further, the call should be made to the undersigned at (416) 863-3164.

Respectfully submitted,

BLAKE, CASSELS & GRAYDON LLP

By _____

John Orange
Registration No. 29,725
Tel.: (416) 863-3164